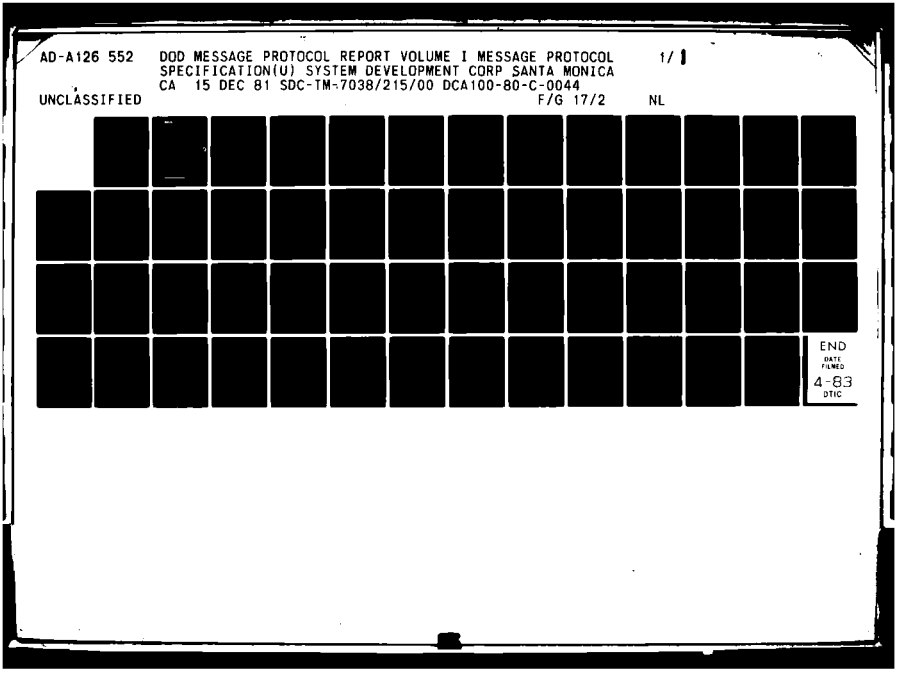
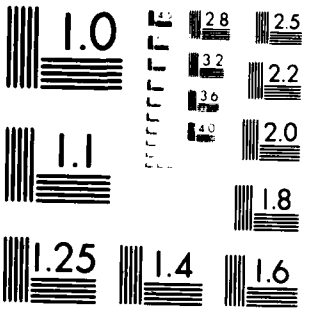

AD-A126 552
DOD MESSAGE PROTOCOL REPORT VOLUME I MESSAGE PROTOCOL SPECIFICATION(U) SYSTEM DEVELOPMENT CORP SANTA MONICA CA 15 DEC 81 SDC-TM-7038/215/00 DCA100-80-C-0044
1/1
UNCLASSIFIED
F/G 17/2
NL
END
DATE FILMED
4-83
DTIC



MICROCOPY RESOLUTION TEST CHART

SDC
System Development Corporation
2500 Colorado Avenue, Santa Monica, CA 90406, Telephone (213) 820-4111

series base no./vol./reissue
TM- 7038/215/00
author
SRI Staff
technical Carl Switzky
Carl M. Switzky
release Carl Switzky
Carl M. Switzky
for
Charles A. Savant
date
12/15/81

TM a working paper

This document was produced by
System Development Corporation in performance of Contract DCA100-80-C-0044

DCEC PROTOCOLS STANDARDIZATION PROGRAM

DoD MESSAGE PROTOCOL REPORT

VOLUME I

MESSAGE PROTOCOL SPECIFICATION

ABSTRACT

The Message Protocol allows the transfer of messages over communications networks. The protocol is divided into the Message Presentation Protocol (MPP), situated at the presentation layer, and the Message Transport Protocol (MTP), situated at the session layer. The MPP supports formal DoD policy concerning the authorization, storage, and release of messages. The MTP supports the transfer of messages between different MPP sites. This document gives for each of these protocols an overview of the protocol, a description of the services offered to the upper layer, and a description of the services required from the lower layer.

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER 7038/215/00	2. GOVT ACCESSION NO. AD A126552	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) DoD Message Protocol Report Volume 1 Message Protocol Specification		5. TYPE OF REPORT & PERIOD COVERED interim technical report 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) SRI Staff		8. CONTRACT OR GRANT NUMBER(s) DCA100-80-C-0044
9. PERFORMING ORGANIZATION NAME AND ADDRESS System Development Corporation 2500 Colorado Ave. Santa Monica, CA 90406		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS P.E. 33126K Task 1053.558
11. CONTROLLING OFFICE NAME AND ADDRESS Defense Communications Engineering Center Switched Network Engineering Directorate 1860 Wiehle Ave., Reston, VA 22090		12. REPORT DATE 15 Dec 81 13. NUMBER OF PAGES 49
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office) N/A		15. SECURITY CLASS. (of this report) Unclassified 15a. DECLASSIFICATION DOWNGRADING SCHEDULE N/A

16. DISTRIBUTION STATEMENT (of this Report)

Approved for Public release; distribution unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

N/A

18. SUPPLEMENTARY NOTES

This document represents results of interim studies which are continuing at the DCEC of DCA.

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Protocols, Data Communications, Data Networks, Protocol Standardization, Message Protocol

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

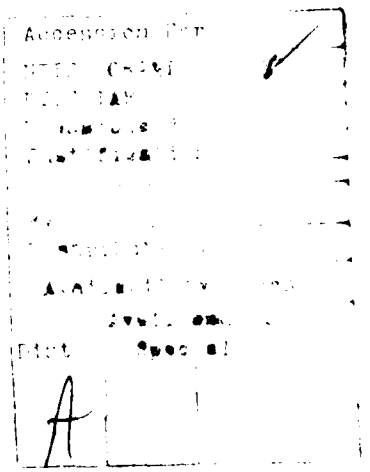
The Message Protocol allows the transfer of messages over communications networks. The protocol is divided into the Message Presentation Protocol (MPP), situated at the presentation layer, and the Message Transport Protocol (MTP), situated at the session layer. The MPP supports formal DoD policy concerning the authorization, storage, and release of messages. The MTP supports the transfer of messages between different MPP sites. This document gives for each of these protocols an overview of the protocol, a description of the services offered to the upper layer, and a description of the services required from the lower layer.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

CONTENTS

LIST OF FIGURES



PART I

MESSAGE PRESENTATION PROTOCOL

1. OVERVIEW

1.1 INTRODUCTION

A computer based message system (CBMS) provides for the creation, editing, formatting, addressing, validation, routing, delivery, and retrieval of messages within and between groups of individuals and organizations in disjoint space and time. A military message system (MMS) must provide additional functions involving security and precedence, authorization and authentication, and interoperability with a variety of existing systems that were designed before the introduction of layered architectures. There is also an important distinction that must be made between formal and informal messages[1]. Informal messages provide a communication channel between individuals, whereas formal messages provide for official, authorized messages between organizations. Furthermore, since multimedia capabilities may eventually be added to message systems, the architecture of the message system should facilitate such enhancements. These requirements, viewed from the user's perspective, are presented in a System Development Corporation document[2] prepared in conjunction with the CBMS specified here.

Previous work on mail systems[3, 4] has led to the decomposition of mail systems into two parts: user agents (UA) and the message transfer system (MTS) as shown in Figure 1. The MTS consists of several message transfer agents (MTA) that cooperate in a distributed environment. During the specification

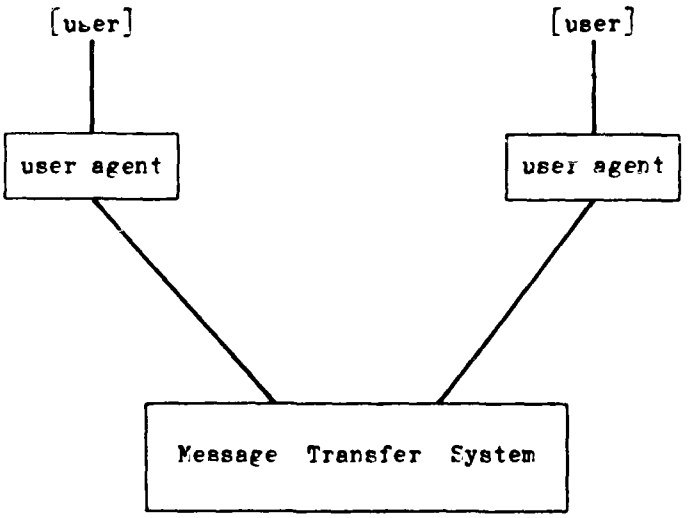


Figure 1. Mail System Architecture in terms of Abstract Machines.

described below, it became apparent that the MTS itself should be partitioned

into two layers as shown in Figure 2:

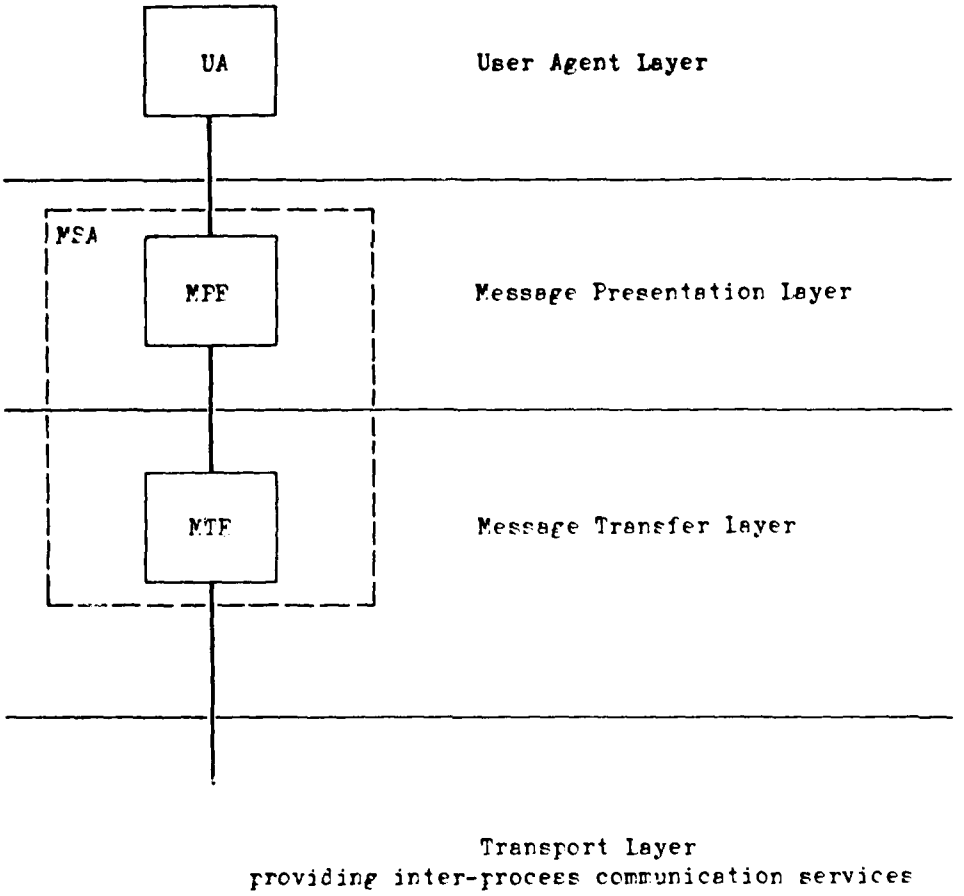


Figure 2. Refinement of the IFIP WG 6.5 CBMS Model

a message presentation layer and a message transfer layer. For this reason, we have written service specifications for two protocols: the Message Presentation Protocol (MPP) for the message presentation layer; the Message Transfer Protocol (MTP) for the message transfer layer. The MPP specification the MTP specification is contained in a related document[5]. In terms of the ISO reference Model[6] and the DoD architecture[7], the MPP resides in the presentation layer, the MTP in the session layer (we assume that existing protocols, such as TCP/IP, are available in and below the transport layer). A justification for this decomposition is given below.

Most existing mail systems (such as ARPANET mail) lack the generality necessary for a high-quality MMS. A good treatment of security, for example, lends itself to the handling of structured messages. For multimedia messages the transfer of structured objects is a necessity, although multimedia services

will probably not be supported in an initial implementation. An adequate model for a message (adequate both for initial implementations and for advanced systems that support multimedia and/or multilevel security) is that a message is a hierarchically structured object consisting of envelopes and data. Envelopes give processing instructions and/or descriptions of their contents. Data are not altered (as regards content) by the CBMS except for format-conversion services necessary to present the data at their destination (e.g., EBCDIC to ASCII conversion). Envelopes may of course be nested. A formalism that expresses this structure has been given by J. Postel[8].

The fields contained in envelopes can be classified according to their use by various portions of the MTS. The MTP, for example, deals with fields containing information appropriate for message transfer. This information generally resides in the outermost envelope, as does the overall security level of the message. Each paragraph of a message may also have its own security level (i.e, each paragraph is contained in its own subenvelope). Such security information may be used in several ways, depending on the level of security supplied by the operating system. At a minimum, it may be used to insert security markings into a document with the aid of a formatting service. The document's overall security, of course, is provided by the outermost envelope; the internal markings (in an environment with minimal security support) have no effect on message transport, access, or storage. Given a more security-conscious environment and a carefully verified MPP implementation, the message system might partition a message, according to the security of each subenvelope, for special handling (to conserve system resources, such as secure links). Appropriate data must appear in the envelope to implement such services.

The structure just described can be extended easily to include to multimedia messages[8]. In terms of transport as viewed from the presentation layer, there is not much difference between multimedia and the handling of classified messages; the major difficulty, rather, lie in handling a wide range of display devices and determining the required grade of service. For example, deciding whether or not to send a graphics message to someone with a particular type of terminal is not really different from deciding whether or not a user may receive a message, given the user's security clearance. Thus, by building the basic notions of nested envelopes into the MTS, a more general system may be designed on the basis of the current work. For the version of the MPP given here, we ignore multilevel-security and multimedia services.

1.2 AN ARCHITECTURAL MODEL

As part of a protocol standardization program, a reference model[7] paralleling the ISO model has been developed for DoD applications. We can fit a CBMS into this model through appropriate placement of the UA, the MPE, and the MTE. Placement of these entities is determined by their respctive functions. UAs serve as an intermediary between the user and the rest of the system: they are responsible for presenting messages to users, storing and retrieving old messages, aiding the user in composing, forwarding, and sending messages, and generally trying to do whatever the user requests.

Because UAs may be tailored to an individual user's requirements, we view them as application-layer processes. The potential diversity of UAs makes verification difficult: thus, they are normally excluded from the "trusted" part of the system. UAs interact with the MTE via the MPE, which is responsible for formal-message authorization, message fragmentation (i.e., breaking messages into separate messages for transmission and reassembling them at their destinations), user authentication, message switching, interoperability with old systems, security, and precedence. Thus, the MPE not only provides temporary storage of entire messages, but also ensures proper and efficient use of the MTS. In many cases, the MPE will pass requests for security and precedence to the MTE. The MTS begins inside the presentation layer and is responsible for all aspects of message transfer.

The MPE is a presentation-layer system. We note that the treatment of formal messages, for example, requires that the mail system maintain control of a message until its release is authorized. If a message requires the authorization of more than one individual, a single UA cannot implement this; the reason is that the message may be presented to several different UAs, none of which can have full control of the message. To display a large message (perhaps one containing graphics or voice) for authorization, one may want to use presentation-layer services such as virtual file systems Similarly, message switching and interoperability may require the use of a virtual file system for temporary storage. As an presentation entity, an MPE is responsible for transferring messages to other MPEs and, finally, to the appropriate UA.

The MTE is a session-layer entity that makes use of services supplied by the lower layers in the system. The MTE supplies services to set up communication channels between various MPEs. It is responsible for obtaining the required grades of service (e.g., security and precedence requirements) from the transport layer. To use the MTE, the MPE invokes presentation-layer services that convert messages to standard formats for transport. This ensures that message representations at one MPE will be mapped into the corresponding message representations at other MPEs. Let us note that standard formats needed for transport between MPEs are potentially useful for other application, and, consequently, belong in the presentation layer. For example, if we use Ada-compatible data structures to represent message formats, a presentation-layer service might map commonly available objects (boolean variables, long integers, etc.) within these structures into the standard representation for each machine (or compiler) in use, thereby allowing one to move MPE software between machines with relatively little effort. (This does not mean that such services do not have to be specified in this document, but rather that they are potentially useful for sub-systems other than the message system.)

For mail system purposes, name servers (NS) are presentation-layer functions (because they need access to a distributed data base). For multiple name servers to maintain a consistent data base, one may wish to use the mail system to do the updates (as in the Grapevine system[9]). This can be done by allowing the inclusion of multilayered objects that consist of two or more entities at different layers with a special interface for management purposes. In general, the upper-level entity is called an administrator (e.g., a name server administrator. [NS Administrator]). Administrators can use the mail system to communicate, and, on the basis of the messages they send, can update

their lower-layer counterparts. An administrator generally responds only to other administrators or to users with special capabilities. Messages received by an administrator from most users can be forwarded to some other user (or an intelligent program) is authorized to carry out what has been requested. If a local NS is not available, an MPE can access a remote NS by using the services provided by the MTEs. The interrelationship of an MTE, an MPE, an NS, a UA, and an NS administrator is illustrated in Figure 3.

The mail system architecture places services not only according to the resources they require, but also in order of message complexity. Thus, the session layer services deal with messages as uniform objects, characterized by various attributes (such as security and precedence), that are to be transported to one or more destinations. Viewed at the session layer, our architecture does not look very different from such existing systems as the ARPANET. At the presentation layer, however, we percieve messages as structures in which various parts of the message may have different attributes. Thus, at the higher levels of the architecture, there is a convenient place to put in a variety of enhanced services, such as multimedia facilities. Because these enhanced services appear explicitly only in the higher layers, it will be relatively easy to add such services while maintaining compatibility with more primitive environments. Finally, the use of administrators for some aspects of system management allows a gradual transition from manual to automatic control of those facilities a user might want to modify (such as the name server).

1.3 SERVICES AND FUNCTIONS

The MPP supplies services that enhance the transfer mechanisms supplied by the MTP. It is assumed, however, that the UA is responsible for providing a friendly user interface, a choice of editors, storage of messages outside the scope of the mail system, etc. Nonetheless, the MPP must provide an interface that supports the construction of high-quality UAs. As seen through the UA's interface to its MPE, the MPP must behave in a regular, predictable manner. In particular, it should be easy for a UA to determine the state of its MPE, especially in the advent of error conditions such as failures of distant hosts. MPP services fit within the following classes:

- o Authentication Services: These allow a user to gain access to an MPE. The identity of the user is verified.

- o Message Creation and Editing Services: These create messages (these may be referenced by symbolic names) and permit the user (i.e., UA) to edit messages (with tools supplied by the UA itself). Creation and editing services also provide for the replacement of individual fields in envelopes in case of an error. In all cases, any actual editting is done by the UA: the MPE only supplies access to the appropriate component in accordance with security, authorization, and formal message policies.

- o Authorization Services: These verify that formal messages have received the required authorization and that they have not been forged. The services also provide for the display of messages to and modification of messages by those users who are allowed to grant authorizations (and also

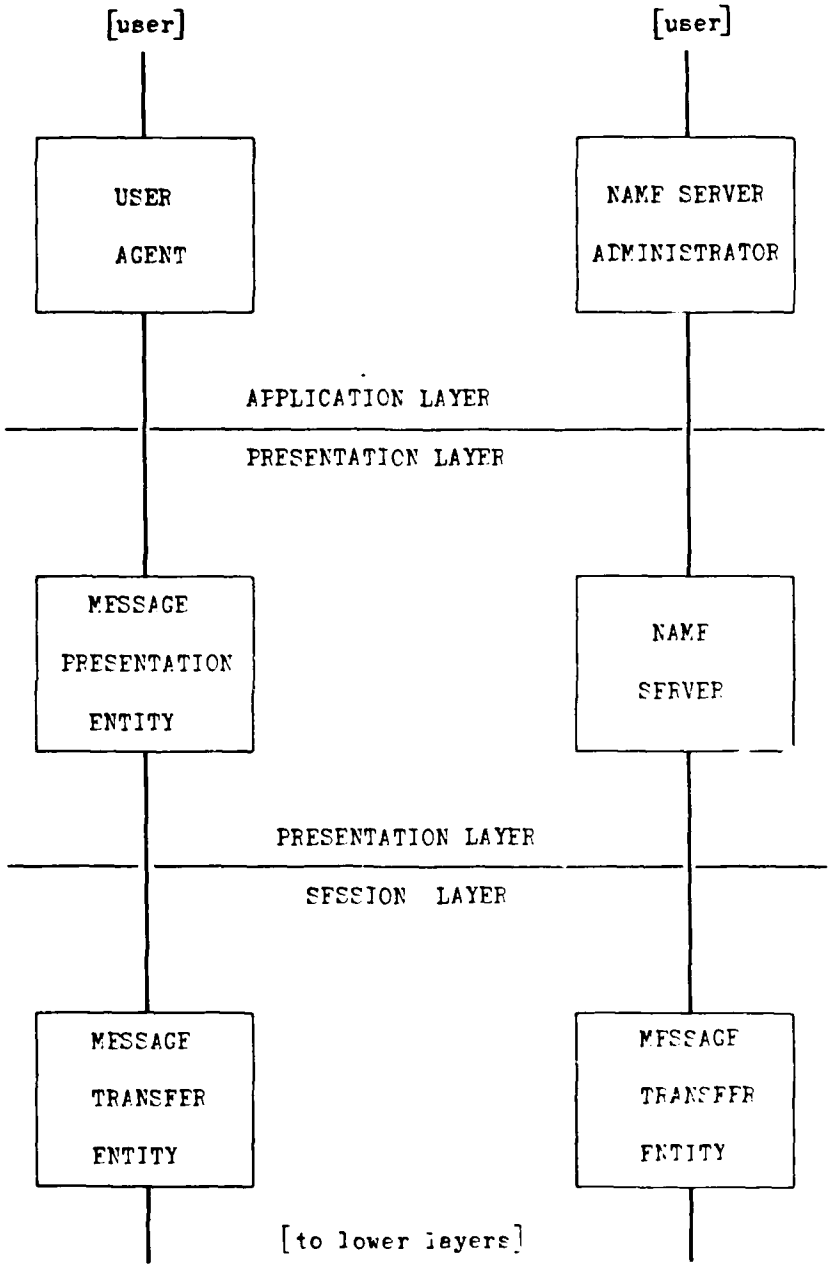


Figure 3. Message Transfer System in Relation to DoD and ISO Layered-Protocol Models

make modifications.) Although modification during authorization is in a sense an editing function (actually done by the UA), the authorization service must control access to the message (i.e., only allow for the modification of certain fields). Some interaction between the editing and authorization services is necessary because of security issues (e.g., the addition of classified material that not everyone in the authorization chain can see), and to allow those individuals responsible for the content of a message to make changes before the message is sent.

- o Naming Services: These allow the user to interrogate NSs. When a message is sent, these services convert the recipient's names to addresses and/or routes for message transmission and name validation. Such conversion is essential for using an MTE.

- o Security and Precedence Services: These verify that the handling of a message does not violate the system's security model and that precedence requirements have been met. Trade-offs between security and delay can be made in conformance with the security model. The quality of the security services depends critically on the underlying operating system.

- o Transfer Services: These transfer messages or message fragments from one MPE to another by invoking lower-layer services. A variety of mechanisms may be used by an MPE to enhance the system's performance. For example:

  - Message Fragmentation Services: These allow the handling of substructures within individual messages. This is done so that links with special capabilities (say, those that are optimally suited to multimedia, or high security) are used only for those parts of messages that need them.

  - Message Bagging: If the same message is to be transferred to multiple recipients using the same MPE, only one copy has to be transferred; the final distribution may be done by the recipient MPE. Similarly, it may be possible to specify a route in which each MPE along the way picks up a copy of the message for local distribution and forwards it. The usefulness of such services depends on the cost of the links in the system as compared with the cost of the nodes.

- o Format Conversion and Gateway Services: These allow one to convert to special formats to drive widely available devices or to conform to standard presentation standards. They also allow for gateways to other networks (such as Autodin I) that may not fit into an inter-networking environment. The actual services may in this case be outside the MPP itself--the MPP may be responsible for ensuring that appropriate resources will be used.

- o Error Recovery: These services aid in error recovery and in the generation of error messages. All MPP services are expected to supply meaningful error messages in the event of a failure, insofar as this is practical. Although an error message stating only that "something went wrong, please try again" may occasionally be necessary, such messages should

constitute only a small fraction of the total number of error messages.

- o Status-Reporting Services: These allow the user of the MPP to determine the location of messages or the state of actions he has initiated. Delivery acknowledgment and status services can be by implemented using a "return postcard" mechanism that informs the sender's message server when the message has reached important points. Return postcards can be constructed from information in the message envelope[10].

The use of such services must, however, conform to administrative policies. Thus, for example, it is not possible to actually send a formal message before the it has passed though an authorization procedure, and a user or UA must be authenticated before being given access to MPP services. Some of the services described above may seem to be local services (e.g., authorization). We have assumed that a given organization may be spread over several separate MPEs, and consequently, any service local to a given organization may be distributed over a communication network.

1.4 A SCENARIO

The following scenarios illustrate the operation of the MPP by tracing the progress of a message through the system.

- o Scenario 1

  1. A UA creates a draft of a formal message with the aid of editing services chosen by the user.

  2. The UA requests that the message be authorized. During the authorization procedure, the message is presented to several other users and is approved by them.

  3. The UA resumes control of the message and sends it. Control of this message passes to the lower layers after successful name-to-address mapping.

  4. The local MPE archives the message (on a local archive).

  5. Archives are stored in system-wide archival facilities for long-term storage. Archival records of envelopes are stored at the originator's and destination's MPEs.

- o Scenario 2

  1. A UA creates a draft of a formal message with the aid of editing services chosen by the user.

  2. The UA requests that the message be authorized. During the authorization procedure, the message is presented to several other users and is approved by them.

3. The UA drafts a second formal message and submits it for authorization while the first is being authorized.

4. The second message is rejected by an authorizing agent (a user with the capability to authorize messages) and returned to the sender with suggestions for changes.

5. The UA resumes control of the first message and sends it. Control of this message passes to the lower layers after successful name-to-address mapping.

6. The local MPE archives the first message (on a local archive).

7. The UA allows the user to edit the second message.

8. The first message is delivered to the recipient MPE and is subsequently forwarded to the recipient user. The recipient MPE archives the message locally.

9. The second message is forwarded in draft form to another user for further changes. The message is then returned to the original sender.

10. The second message is then resubmitted for authorization.

11. The message is approved after the modified message has been compared to the original version.

12. The message is then sent.

13. Archives of both messages are stored in system wide archival facilities for long-term storage. Archival records of envelopes are stored at the MPEs of both the originator and the recipient.

o The following scenarios assume that archiving is done implicitly (as shown above); transmission and delivery conform to the preceeding scenario.

o Scenario 3

1. A formal message is drafted by an unclassified user.

2. The message is submitted for authorization. In the process of authorization, a classified paragraph is added, thereby changing the security level of the message.

3. The message is sent without review by the originator because of security considerations.

o Scenario 4

1. A formal message is drafted and submitted for authorization.

2. The message is not authorized within the time allowed by the authorization rules.

3. The originator (who, in this case, is allowed by administrative policy to override authorization procedures) overrides the authorization procedure and appends an explanation as to why he did this. As part of the envelope, the message contains a warning that the authorization procedure was bypassed.

o Scenario 5

1. A formal message is drafted, authorized, and transmitted.

2. It arrives at a destination MPE.

3. The message is forwarded to a mailbox for high-precedence messages.

4. The message is passed to the recipient UA.

2. SERVICES PROVIDED TO THE UPPER LAYER

This section describes the services that are provided by the presentation layer. Various services are considered: message creation and editing, naming, authorization, transmission, archiving, and status reporting. In addition to the services described below, various sites or facilities may offer enhanced services. This is appropriate for information-request services. Some hosts, for example, may allow one to obtain from the NS the route along which a message will be transferred, various information about users or organizations, and so forth. If a request for services is not supported at a particular site, the service should reject the request with an explanation as to why this was done. NS responses must be mutually consistent, so as to support a good user interface.

2.1 MESSAGE-CREATION AND EDITING SERVICES

It must be possible for a user to create, store, and edit entire messages and fragments of message text that can subsequently be inserted into messages. While a message is being created, it must be possible at any time (right up to the final commitment to send it) to display the message and edit it. The UA supplies the actual editors; the MPE only gives the UA access to message components.

2.1.1 Simultaneous User-Agents

It should of course be possible for the message system to support user-agents working on behalf of simultaneous users, except on single-user dedicated processors.

2.1.2 Simultaneously Active Multiple Messages per User-Agent

A single user should be able to work concurrently on more than one message. He should be able to act on catalogued messages that have been previously received, e.g., to forward or answer them. He should also be able to work with multiple messages at various stages of preparation. For example, from inside the SEND mode of the message system he should be able to save and restore messages in progress, working on them in alternation as desired and necessary

2.1.3 Forwarding Formal Messages

It may be desirable to forward formal messages (i.e., to include copies of these within other messages.) It must therefore be possible to place a read-only copy of a message within another message. The protocol ensures that this copy is not altered during editing or transmission. The message envelope indicates whether a copy of a cataloged message is included.

2.1.4 Error Handling

The system design, by providing sensible diagnostics, warnings, and prompts, should anticipate all the likely errors a user might make. For example, if a local name is invalid, there might be an immediate refusal of that name--but

this would never cause rejection of an entire list of names. It should be possible to edit a name in the middle of a name sequence, or to edit any unprotected field, such as the SUBJECT field. (Note that all such modifications must conform to the established security and authorization policy.)

2.1.5 Format Conversion

Some UAs may wish to use local formats for message presentation or editing. Local formats that may be supported (on a site-by-site basis) include JANAP 128, ACP 127, ACP 126, and DOI 103. In some cases, variants of these formats are to be supported rather than the formats themselves. For example, JANAP 128 uses two RETURNs and a LINEFEED to separate format fields, because the extra RETURN does not print and is therefore invisible to the user. Some file systems or editors may be confused by this convention; consequently, an implementer may prefer to use a JANAP 128 look-alike (if he wishes to utilize existing facilities).

2.1.6 User-Supplied Envelope Fields

The user of the protocol must supply a name together with a precedence level for each recipient (only the ACTION or TO fields are required) and a security level for the message, whether formal or informal, plus an authorization key for formal messages (this will be described below); all other fields are optional.

The following optional fields may be used by other MPP services:

- o INFORMATION or CC Fields. These allow for the transfer of additional copies of a message to recipients.

- o ATTN Key This field supplies keywords that may be used by recipients for internal distribution. An ATTN key allows the establishment of temporary keywords to expedite distribution of messages within recipient organizations to offices that deal with particular tasks.

- o Archival Keys This field allows the user to supply keywords for archival and retrieval.

- o Accounting information Some organizations not directly related to the DoD may have access to the mail system. Such users must supply accounting information so that they may be charged for the system's use.

- o Multimedia Although multimedia messaging will probably not be supported in the initial version of the message system, when (and if) such services do become available, information must then appear in the envelopes describing the type of media, and how they are to be handled. These services also apply to multilevel security. Such structural information might include

    - The type of media

- The security level for a message substructure

- The synchronization and/or ordering of the media

2.2 NAMING SERVICES

In this section, we describe the naming services provided the user agents. Naming services entail the provision of attribute information for a given name. The names supplied by the UA are assumed to be uniform in format. Any incompatibility in naming conventions for different communication environments is assumed to have been resolved by the user agent. A given name may have associated with it several attributes of interest to the protocol user. Examples of such are security classification, organizational affiliation, multimedia sophistication, and whether formal or informal messages can be handled. Administrative policies can control access to these attributes on the basis of a user's capabilities (e.g., it may not be desirable for an unclassified user to know the top classification level that other users in the system may have). also provided are services for information retrieval and validation, for creation, modification and deletion of name entries and information. The naming services at this level are machine-oriented, with those that are user-friendly being furnished by the user agent.

2.2.1 Names, Distribution Lists, and Set Operations

Naming conventions must be the same at all sites in order to provide for remote access to a variety of NSs. In addition, naming conventions must be compatable with current standards such as the DoD organizational names used by Autodin I. For this reason, the conventions described below suggest uses for various characters.

Names in their simplest form are represented as strings of letters, digits, ampersands (&), underscores (_), periods (.), and dashes (-). For convenience, all of these symbols will be referred to as literals. In addition to individual names, the protocol supports distribution lists (sets of names that are to be included in one field of a message) and set operations on these lists. There are two classes of service:

- o Distribution list expansion. A distribution list contains individual names and the names of other distribution lists in an arbitrary order. A maximum level of nesting for distribution lists is necessary to prevent looping. A maximum of five levels is suggested. For message delivery, the UA may provide a prospective combination of individual names and names of distribution lists. Such a combination may be in list form or may be given by means of set operaions.

- o Set Operations. The set operations allow union, intersection of distribution lists, inclusion of individual names with distribution lists, or exclusion of individual names or distribution lists from a distribution list. Such a combination provided by the UA is expanded into a list of individual names. In case this naming combination is supplied for address mapping, its expansion into individual names is first executed before the name-to-address mapping for each name is performed. The

following symbols are reserved for set operations: "^" for intersection, "," for union (because this delimits individual names), and " " (as a binary operator) for set difference. The symbols "{" and "}" are reserved for delimiting sets. These symbols were chosen because they are not likely to appear in any reasonable name.

If a set or distribution list is not available at the initial name server or some other name server along a route, it may not be possible to perform intersections or set differences. In this case, all users who are not positively excluded will receive the message.

In addition to names specified by distribution lists and/or set operations, the NS supports aliases and generic names. An alias is an alternative symbol representing a name. For example, the routing indicator of AUTODIN I may be included in the NS as an alias to maintain compatibility with previous practices. Aliases are replaced by the name with which they are associated when the NS is invoked. Generic names are expressions that indicate lists of names. The special symbols, "[", "]", "*", "?", and "'", appear in generic names. The symbols "^" and "-" can appear only within square brackets. Generic names can appear only in information requests to a name server, not when called by transmission services. Generic names are interpreted as follows (the notation is patterned after the UNIX file system conventions):

? represents any literal.

* represents any number of literals including 0. The letters may be different

[<String>] stands for any of the literals specified by <String>. Two literals separated by a "-" represent those two letters and all intervening ones in the ASCII ordering. A "^" just after the "[" indicates that any letter is valid except the ones specified in the remainder of <String>.

For search purposes, letters are taken to be case-independent from A-Z, digits 0-9, "&" (the ampersand),"_" (the underscore), ".", and "-" in that order. Not all name servers are expected to support generic names; however, they must all return an appropriate error indication if generic-name symbols are seen but cannot be handled.

2.2.2 Name Creation and Modification

Updating services allow authorized users to create or modify name entries and the information associated therewith. The naming convention used allows the distribution of naming authority. Each NS authority has a jurisdiction that allows an individual organization to have its own naming authority. Every Name Server has a name-server administrator (with a mailbox) with the authority to make changes in the data-base. Special user agents may be allowed to alter the data base even if an administrator is not actually logged in. These user agents must be authenticated (this facility allows some of the NS administrator's functions to be eventually automated). We emphasize that only the NS administrator or special UAs under the administrator's control can

alter the data base. Because any changes in the name server must be approved, the message authorization service can be employed for this purpose. For example, one possible scheme is to have a request for entry modification sent as a message to be authorized by the appropriate agent. Upon approval, the message is forwarded to the NS administrator (or to his user agent only). Services to modify the data base can then be called upon. A log must be kept of all modifications and end users notified of any change that affects them. In the event of a change of address, the notification is to be sent to both the new and old mailboxes.

2.2.3 Name Searching and Validation

Name server information retrieval services are provided the user. They allow a UA to obtain a list of names that satisfy simple search criteria (i.e., any set of names that may be formed by set operations, distribution lists, and generic names) and to see various attributes associated with each user, such as his level of security clearance. These attributes, however, may be selectively protected from general access on a name-by-name or attribute-by-attribute basis. If some attribute cannot be seen, this fact may be noted. The naming information furnished for the purpose of message transfer is validated automatically without any special request.

2.2.4 Name Searches on Remote Name Servers

Normally an MPE accesses a local or nearby name server. If desired, one may access a distant name server to obtain more detailed data than what may be available locally. This service allows one to specify a remote name server: it then supplies any of the naming services available on the remote host that are with the remote facilities policies for access of its database.

2.3 AUTHORIZATION SERVICES

A formal message must be authorized by authorizing agents (individual users who are permitted to authorize messages), before it can be sent. Manual authorization procedures usually require signatures, either sequentially or in parallel, from a number of individuals. In many cases, any one of a number of individuals may authorize a document for release; but if a question arises as to who should authorize a given document, the system may provide someone to ask. Furthermore, there are normally administrative controls to prevent the release of unauthorized messages.

Authorization services mimic these manual procedures. Authorization services belong in the MPE for several reasons: messages must be shown to multiple of users (a presentation function), each with limited capabilities for modifying a message; these users may be on separate hosts thereby requiring network resources; finally, in a computer-based environment, the easiest way to ensure that an object will be handled according to some rule (regardless of what the user tries to do) is to place the object under the control of an independent process.

A major difficulty in designing effective authorization services is the handling of exceptions. Such services should prevent misuse of the message

system and be flexible enough to handle unusual situations (e.g., what to do if no one who can authorize a message is available). Authorization services provided by the MPE can grant or deny the ability to change a message to authorizing agents, can handle multiple authorizations (either sequentially or simultaneously) and can optionally resubmit a message for authorization when changes are made. In all cases the authorization service indicates how a message has been handled. For instance, if a message has been changed (e.g., a classified paragraph has been added) and sent (by authorizing agents only) without being resubmitted to some previous authority (e.g, someone who has already approved the message, but is not cleared for the classified paragraph), the originators and recipients are notified accordingly. The service always verifies that the authorizing agent can authorize the message. Authorizing agents may frequently be the individuals ultimately responsible for the contents of messages--the "senders" may be part of these agents support staffs--and consequently some interaction between the editting and authorization services is necessary.

Occasionally, becasue of heavy work overloads, system degradation, etc., an important message may not go though the authorization process fast enough. Since it is important in real applications to handle such situations gracefully, there is a way to override the authorization service. If an authorization is not granted within a reasonable time (which has to be specified to the authorization service), an override is possible. The sender (if granted this capability) can request that the message be sent anyway; however, the MTP will indicate that this is being done, and the time allowed for authorization will be included in the message. If the message has been rejected by an authorizing agent within the time interval for authorization, the override (to send) is prohibited.

2.3.1 Authorization Rules

Authorization rules (the statement of authorization policy that the MPE is to follow) must be set up before formal messages may be sent. These rules allow one to select authorizing agents on the basis of criteria involving the sender, recipient, security level, precedence, and/or authorization key of a message. (Authorization keys are keywords that are used to classify messages according to the sending organization's criteria has for internal use.) The authorizing agents selected may be called by the service sequentially or in a random order, on a first-available or plurality basis (only a fixed number of rejections by agents is permitted). Any authorizing procedure (the prescribed sequence of events a particular message can be authorized) can be specified by using both logical and temporal relations. Each individual message, however, is presented to only one authorization agent at a time. In the event of a rejection, modification, or request for change, the message may be resubmitted for reconsideration along the chain of agents chosen by the authorization procedure.

2.3.2 Classes of Authorization Services

There are three classes of authorization services: those that change authorization rules, those that apply them, and those that request information about them.

2.3.2.1 Services that Modify the Authorization Rules

An authorization service data base is initialized and maintained by services that modify the authorization rules. Authorization services must authenticate all users who attempt to modify the data base, and must report any changes in the data base to appropriate users.

To modify the authorization rules, an appropriate user can either replace them, or insert new ones at special access points. Replacement of the rules by a small number of trusted personnel is generally allowed. More than this number may be permitted to modify the authorization rules at the access points. Such modifications, however, are restricted to insertions--and the statements that can be inserted into the rules may be restricted at any given access point. The restrictions are explained in more detail in Appendix A.

The service that modifies the authorization rules performs the following functions:

- o User name authentication. The service must make sure it knows the name of the user who is to change the authorization rules.

- o Access name search. Each access point has a corresponding access name, which the user must give if he wishes to insert rules at an access point. The service then checks the list of users allowed to make changes at this point and verifies that the current user is included. If no include-name is given, the user must then be validated against a list of those users who can make changes in any of the rules.

- o Syntax check. The service checks the new or modified inclusion rules for syntax and allows them to be accepted only if the syntax is correct. In the event of a syntax error, the service returns an indication of what the error was.

- o Modification or Creation. At the request of an authorized user, the service will create new authorization rules if none were previously available, and will replace the old rules if rules already existed. A message will be sent to appropriate users indicating what changes have been made. If changes were made by means of an include statement, this fact will be noted in the messages.

2.3.2.2 Services that Apply the Authorization Rules

To apply the authorization rules, the UA intending to send a message must invoke the authorize service. The latter searches the authorization rules for a valid authorization procedure, which it then uses to obtain the authorization as follows:

- o The authorization procedure continues as long as each agent in turn authorizes the message or declines to handle it. If a message is explicitly rejected by an agent (or a group of agents), the message is returned to the sender with a notification of the rejection and perhaps an explanation supplied by the authorizing agent. If the message is

modified, two courses of action may ensue:

- The message may be returned to the sender or to the authorizing agents that preceded the current authorizing agent. Unless explicitly aborted, the authorization procedure is repeated with the same authorizing agents as before, and in the same temporal sequence.

- The message is passed along, but the fact that the sender has not seen it or that other authorizing agents have not seen it is noted on the message. (This is necessary if, for example, a secure paragraph must be added, when not all of the users have been cleared.)

o If a message is passed though the authorization process more than once, an authorizing agent may review any version of the message. Ideally, one should be able to see each version or the changes between versions.

o If a message is not authorized within the alloted time and no alternative authorization procedure is specified in the authorization rules, the sender is notified (with a status message). If the sender has the authority to override the authorization procedure (when the time limit is exceeded), he may take one of three courses of action:

  He may have the message sent. It then includes a warning that the authorization procedure has been overridden and states what the time limit was. All authorizing agents are informed of the override. The originator may append an explanation as to why he bypassed the authorization procedure. This explanation is set apart from the main body of the message.

  He may purge the message (i.e., remove the message from the mail system). If this is done, all authorizing agents are notified.

  He may do nothing, in which case the authorization process continues.

  The authorization service maintains a history of the authorization procedure. A complete record is kept, but is available only to the originators and authorizing agents. An abbreviated record, appended to the message as seen by the recipient UAs, includes only the final part of the authorization chain determined by local administrative policy.

2.3.2.3 Services that Supply Information

The user can ask the following questions:

o Given an authorization key, recipient, and sender, what is the authorization procedure?

o What are the current authorization rules?

o Who is notified of changes to the authorization rules?

o Who can modify the current authorization rules?

o Who is allowed to invoke the "include" facility?

At any MPE, the system administrators may deny a request or restrict it to various classes of users. In such a case, the information service issues a standard error message indicating that the requested information is not available.

2.4 TRANSMISSION SERVICES

The main transmission service transmits a single self-contained message from a user agent to one or more others. There are also services to meet specific transmission-related needs. Some of these may be optional, but others are essential to meet system goals, such as reliability.

Depending on whether a UA is an originating user agent (OUA) or a recipient user agent (RUA), it will use different services. Posting services are offered to the OUA, delivery services to the RUA.

A military environment has two types of messages: formal and informal. The formal messages, when presented to the user, have specific formats, such as JANAP 128, ACP 127, ACP 126, and DOI 103. Formal messages are exchanged not between individuals, but between organizations. Formal messages also require services specifically designed for military message systems--especially precedence, authentication, authorization, and classification. The informal messages are exchanged directly between individuals. Authorization does not apply to informal messages, although security and precedence may. Since, however, the main role of a military message system is to exchange formal messages, the latter should get higher priority when resources are limited.

The transfer service appends the following information to a message envelope for use by the recipient:

o A time stamp and message ID

o The OUA

o The organizational affiliation of an OUA if the message is formal

o The route the message followed in reaching to its destination.

2.4.1 The Posting Services

After the message has been put into a transfer format and the fields validated, it is posted. A posting service starts the transmission in accordance both with the OUA's request and with administrative policy. A posting servioe informs the OUA that it has assumed responsibility for the message. The OUA is then free to do other tasks, including deleting his record of the message, if he chooses.

If, for any reason, the message cannot be transported or delivered as requested, the OUA will be sent an error message describing the source of the problem and possibly the nondelivered message as well.

2.4.1.1 Formal-Message Posting

The user can request that a formal message be sent. The posting service ensures that the message has been authorized. If it has not, the authorization services must then be invoked automatically.

2.4.1.2 Drafts of Formal Messages

Drafts of formal messages may be passed between individuals (working in a distributed environment) for modification before the messages are actually sent, even after a rejection by the authorization process. Formal messages may be conveyed to any user as long as this is consistent with local administrative policy (e.g., organizations may restrict the dissemination of formal messages among their users).

2.4.1.3 Routine, Urgent and Timed Delivery

The user of the MPP can request a variety of delivery options, depending on the ugency of delivery and the special acknowledgment required. There are five precedence classes (although some may be used only by formal messages in accordance with administrative policy): ECP/CRITIC, FLASH, IMMEDIATE, PRIORITY, and ROUTINE. If no delivery options are specified, routine delivery is assumed.

All deliveries must attempt to meet system goals for reliability, security, and performance. Each class has a prescribed time limit, for delivery of the message The major delays are transfer delay (from the originating MPE to the recipient MPE) and delivery delay (from the recipient MPE to the recipient UA). If the transfer delay exceeds the prescribed time limit, the message is considered undeliverable and an error message is returned to the OUA and other recipients. If the message has been delivered to the destination MPE, but the total delay exceeds the limit for the message's precedence class, the destination MPE decides (on the basis of policies pertinent to that site) whether or not the message is to be delivered. If the destination MPE delivers messages whose time limit has expired, it must warn the recipients. In any event, the originating MPE is informed of whatever course of action is taken, and this information is available to the user of the MPP.

In addition to restricting the delivery time for each precedence class, the user could request that a message be delivered no sooner or no later than a specified date and time. Here too, if delivery cannot be accomplished as directed, an error message will be sent back to the originator and made available to the user of the protocol.

2.4.1.4 Multi addressing

Messages may be sent to multiple users who are named by using the naming conventions in the section called <NAMING SERVICES>, except that generic names are prohibited. Any name (or set of names) may be given a precedence level for messages destined to that name. The user may also place names in one of two fields: an ACTION (or TO) field or an INFORMATION (or CC) field.

2.4.1.5 Routing

If desired, a route may be specified for a message. This route may in turn specify only the intermediate MPEs, thereby allowing the originator to avoid the queueing of messages at sites the originator believes to be possible unreliable. In general, the use of this option will prolong the delivery delay, but it may forestall message interception if the physical security of a host (located along the normal route) is suspect. Routes may be specified on a recipient-by-recipient basis. Utilization of this facility implies some knowledge of network topology.

2.4.1.6 Delivery Acknowledgment

The more important a message is, the more concerned will an originator be about its fate. The following events are of particular interest:

1. Arrival of the message at the recipient MPE(s), ready for delivery to the recipient UAs.

2. Actual delivery to the recipient UAs.

3. Viewing of the message by the recipient(s) and other addressees.

4. Reading and comprehension of the message by the recipient(s).

The first three events can be monitored by the message system, while the fourth is best left to the recipients, who can to reply as needed.

The originator can request that he be notified of any or all of the first three events: message arrival (including arrival at intermediate MPEs, if desired), message delivery, or the fact that the message has been seen. Monitoring each event requires the cooperation of peer entities in the distributed message system. Notices regarding message arrival, delivery, and the fact that the message has been seen, respectively, are sent by the delivering MPE, the recipient MPE and the recipient UA.

As with postal mail, acknowledgments and notice of delivery are not often necessary. Most customers need no more than to be notified of undeliverable mail. The maximum delay time described above avoids the postal mail uncertainty of not knowing wheter a message has been properly delivered.

2.4.1.7 Delivery Cancellation

The originator can request that a previously posted message be cancelled. Although the request may be too late, the message originator will be notified of the success or failure of the cancellation attempt. If the attempt succeeds, the originator can request a copy of the cancelled message. It can then be changed and resubmitted.

2.4.1.8 Secure Transmission of Classified Documents

The transmission service ensures the integrity of messages only during transmission. The security of message preparation and access is controlled by other services. (This topic requires further study.)

2.4.2 Delivery Services

2.4.2.1 Duplicate Detection and Removal

The delivery service detects and removes duplicated messages. Although the mechanisms used by the message transfer service can be expected to minimize duplicate transmissions, these mechanisms cannot be expected to be totally reliable. It is acceptable to limit the time interval for message arrivals during which message duplication will be checked. Such a limit should be long compared to the mean transfer delay for messages, thus making it highly probable that duplicates will be detected.

2.4.2.2 Delivery Schemes

The recipient can choose a delivery scheme. Typically, the recipient MSA stores each message until it is requested by the UA, which allows the UA to present messages to the user at his convenience.

Although convenient for the user, this delivery scheme does not deal well with urgent messages. Rather than waiting passively for the user to check for messages, the message system should notify the user of the arrival of an urgent message, preferably without interrupting work in progress. Such intevention requires the cooperation of the process to be interrupted. Notification can be either visible or audible. Even closer cooperation would allow a high-precedence message to be displayed immediately.

2.4.2.3 Receipt Order Selection

Independently of the mane in which messages are delivered, the recipient can select the order of message presentation. How messages are presented depends upon such factors as their type (formal or informal), urgency (precedence/priority), originator, subject, and time of receipt. Thus, the user could choose to view formal messages before informal ones, higher priority before lower, or messages from superiors before those from subordinates.

2.4.2.4 Receipt Sorting

The delivery service may deliver messages to different mailboxes on the basis of the message's security, precedence, and/or ATTN (attention) keyword. This is especially useful for formal messages in that high-precedence or high-security messages can be delivered to different personnel than normal messages. The delivery service allows the user to set these options or to see them.

2.4.2.5 Other Delivery Services

As noted above, a recipient may have several alternative addresses (mailboxes) for reasons of either convenience or reliability. Alternative addresses are maintained for the name server by a name administrator.

Automatic forwarding is very similar to its postal analogue. The recipient can specify how long the address change is to stay in effect.

2.5 ARCHIVING SERVICES

It must be possible to store any message in a highly reliable, permanent form--and in such a way that it can subsequently be retrieved. Archiving is thus useful both for maintaining historical records and for ensuring the presence of reliable backup copies in case of the primary copy is lost (although it may take time to retrieve the backup copy). Such services should be available either on a default basis (e.g., for all formal messages, or for any message that remains undeleted after some settable period of time, say a day or a month), or upon demand. There should be an option at the time of the archive request as to whether a message will disappear from the on-line message catalog or remain active. The default should be user-specific. It should also be possible to archive messages either singly or in groups.

2.5.1 Archiving Policy

The archiving service at a given MPE may implement archiving policies that are appropriate to that site. These policies may, for example, require that all formal messages be archived, that informal messages be archived only on local hosts, or that informal messages be archived by local hosts only, using system-specified facilities.

2.5.2 Archiving on Local Hosts

The actual archival storage may be local or centralized, as desired. In some cases local archiving will be essential, e.g., because the central facilities are not secure or because retrieval delays are not acceptable

2.5.3 Archiving on Remote Hosts

In many cases, local hosts will not have sufficient capacity and adequate reliability to provide archiving services. In such cases, archiving on remote hosts should be essentially indistinguishable from archiving on local hosts, except that the user must be made aware that the archiving is not being done locally.

2.5.4 Cataloguing and Retrieval of Archived Messages

The cataloguing of archived messages should be consistent with the cataloguing of active messages. Essentially any operation that can be performed on the catalog of active messages should be possible on the catalog of archived messages. For example, it should be possible to request a list of all archived messages with a given subject string, KEYWORD field, message ID/time stamp

(this is unique to each message), TO or FROM field strings, and to retrieve all messages or just selected ones in such a subset. The catalog of archived messages and the requests for retrieval are presumably accessible from within the message system.

Envelopes may be archived in addition to messages. All the archival services apply to envelopes as well; however, envelopes would normally be archived on local hosts only.

2.5.5 Security Considerations

It is important that archival services be integrated into the design of the message system, e.g., so that these services are accessible from the message system. It is expected that the archive requests and those for the retrieval would both be integral parts of the message system itself.

Furthermore, the archival services must conform to the established security requirements. For example, it should not be possible for one user to access another user's archived messages, unless that is the explicitly established policy. All formal messages must be archived. However, if there are messages whose protection indicates DON'T ARCHIVE, this injuction must be observed.

2.6 STATUS-REPORTING SERVICES

2.6.1 Acknowledgements and Processing Status

As in postal mail, the sender of electronic mail may require some assurance that his message has safely reached its destination. The absence of either a returned message or some other error indication often results in confusion (for the user) because of the variability in delivery across a network (even more so, because of the variability across interconnected networks). Delivery acknowledgments and status requests are the electronic mail analogues of "return receipt requested" and delivery status checks, respectively.

In most existing mail systems the sender is notified by his mal server or mail transport protocol. when his message has been posted. The user, however, may also be concerned about the fate of his message at other points:

1. Arrival of the message at the recipient MPE, delivery to the recipient UA.

2. Actual delivery of the message to the recipient UA.

3. Viewing of the message by the recipient.

4. Reading and comprehension of the message by the recipient.

In checking on the status of a message, the user may also be concerned about how far along his message has progressed.

5. When it has been handled by intermediate MPEs.

At each of these points, the user is concerned with knowing whether the message has reached the next point and ifnot, the reasons therefor (e.g., faulty address, host unavailable, connection broken, message not deliverable in time, or message discarded because of system overload). All but the last of these conditions must be monitored by the peer or supporting entity responsible.

The sender can request two kinds of acknowledgment services: to be notified automatically of any of the above conditions or to check the status of a particular message delivery. To obviate network wide searches, the mail system need honor these requests only if the user asked for the additional service at the time the message was sent.

Delivery acknowledgments and status requests are particularly helpful for formal messages, which must be approved by a series of coordinators and authorizers before they can be released. The authorization procedure requires signatures, either sequentially or in parallel. A status request for a formal message informs the user where in the coordination and approval process his message is--who has signed off and "on whose desk" the message is now located. More sophisticated status requests could include approval dates, any deadlines, and whether the message has been changed (e.g., to add a classified paragraph).

2.6.2 Automatic Status Reports for Error Conditions

In the advent of an error, the user must be informed of the status of the service that he had requested.

2.7 MISCELLANEOUS SERVICES AND OPTIONS

A number of services and options may be available on a given CBMS that have not been explicitly mentioned and are not strictly necessary for mail system use. The basic services described earlie, however, may help in implementating such extensions. Envelope archives, for example, might be required for certain users (e.g., non-DoD users, who would pay for their use of the message system) because the envelopes could be used to estimate costs for accounting purposes. The local NS is an ideal place to store the data needed to identify such users. Similarly, a particular MPE may have administrative restrictions on the way in which users can make use of the mail system, what is to be archived locally, for how long, and the like. Any such additional services, restrictions on use, or options, however, should affect only local users; there must be no constraint upon the behavior of the system as seen by users not subject to the administrative authority. Any restrictions on the receipt of mail (e.g., prohibiting informal messages) must be indicated in a NS's data base and the existence of such restrictions explicitly recognized in the overall policy of the system.

3. SERVICES PROVIDED BY THE LOWER LAYER

The MPP is built upon message transfer protocols residing in the session layer. An MPE may use the services of several distinct session-layer entities running the same or different protocols, thus allowing multilevel secure systems to be built on top of lower-layer protocols (such as TCP) that require similar security-levels for all peer mutually connected protocols. The ability to use multiple session-layer protocols also allows the message transfer system to use multiple networks that are not directly interconnected. This allows interoperability with systems (such as Autodin-I) for which a direct physical connection is neither desirable nor permissible (say, as a matter of policy).

3.1 VALIDATION SERVICES

Because the actual transfer of messages is done by the lower layers, there must be assurance that only a legitimate MPE will use these layers for mail system purposes. This is necessary to prevent (for example) a user agent from bypassing the administrative controls supplied by the MPE. Similarly, each session entity must know the identity of the peer entities with which it communicates, and must ensure that they are authorized for mail system use.

3.2 AUTHORIZATION SERVICES

Although formal-message authorization is primarily an MPE function, some support from the lower layers is necessary, as authorization may require the coordination of several MPEs.

3.3 TRANSFER SERVICES

Transfer services when provided with the internet addresses of MPEs, move messages from one MPE to another. The basic service is a "send" service. The "send" service must be given a message with an overall security level, a precedence level, and a list of recipients. As viewed from the lower layers, each recipient consists of a security level, a precedence, and a series of alternative addresses (one or more). The service attempts to send mail to the first of these addresses, trying the second one only if mail cannot be delivered to the first--and so on through the entire series, if necessary. The MPE address given to the service is not necessarily that of the recipient; however, if a message is to be passed farther along the network (i.e., to another MPE), this is the responsibility of the MPEs, not the MTP.

A "send" service can be invoked with a variety of options:

- o Normal Transmission. A message is transferred through a reliable transport mechanism to a remote MPE.
- o Source Routing. The user of the protocol may specify the route with whatever level of control the transport mechanism allows.
- o Error Conditions. If none of the MPEs specified in the address list can be reached, or if there is a failure during transmission from which the

lower layers cannot recover, the "send" service returns an error indication to the user of the protocol.

- o Security. The lower layer checks that the security level requested for a message matches that requested from the transport mechanism.

- o Precedence. Several precedence levels may be specified. These include ECP/CRITIC, FLASH, PRIORITY, ROUTINE.

3.4 NAME-SERVER ACCESS SERVICES

This service allows access to remote NSs. The MPE may request services from a remote NS, but may not make changes in the NS's data base. If a remote NS cannot be accessed, or if there is a failure, appropriate error indications are returned.

3.5 STATUS-REPORTING SERVICES

Status-reporting services allow for the transfer of delivery acknowledgements and status messages between MPEs. Different grades of service may be requested, depending on whether or not occasional loss of one of these status messages is acceptable.

3.6 ARCHIVE-ACCESSSERVICE"

Archive access services enables an MPE to connect with a remote MPE to access the latter'a archival services. These services allow one to request services from remote archival facilities; i.e., to retrieve archived messages or to interrogate an archive's data base when that archive is not available on a local host. Generally, these services are used to access long-term archives, such as those that might be maintained at a central facility.

4. APPENDIX A

Authorization procedures and authorization rules can be described with a formal grammar. These procedures can be constructed from authorizing agents with the aid of logical and temporal operators. In terms of standard logical operations, "and" implies that both of two agents must approve a message, while "or" implies that, if either approves, the message is authorized. An authorizing agent can either approve a given message, reject it, or pass (refuse to act upon it). From a logical standpoint, an authorization is treated as "true" and "pass" is treated as "false". The authorization procedure continues until it logically becomes true or an explicit rejection occurs, which then results in termination of the authorization process. Normally just one rejection terminates the procedure; however a different number may be given explicitly (this option also applies to individual parts of an authorization procedure).

In addition to the strict logical operators "and" and "or," one can exert temporal control over an authorization procedure. This is done with the "and_then" and "or_then" operators. These are logically identical to "and" and "or," respectively, except that the agents must approve a message in sequential order. There may also be time constraints on authorization procedures that give alternatives to follow if the constraints are not met. If there is a time limit and no alternative authorization procedure, the sender of the message may override the authorization rules (if the user has this capability). Otherwise, the process continues until the whole authorization rule becomes "true" or a time limit is exceeded.

A given authorization agent can be granted the explicit authority to modify a message, or a restriction that prevents him from modifying a messages. If modification occurs, the authorization process may be restarted (if not, anyone who has not seen the current version may have this fact noted by the message system). If a message is modified, the MPE can show the user not only the various versions but also the changes between versions--unless this results in a conflict with security policies (e.g.,if a classified paragraph is added during the authorization procedure, a sender without a security clearance cannot see this part of the message).

A broadrange of authorization rules may be supported by the MPE. Because the authorization facilities are complex, we shall specify these a by using a context-free grammar. This grammar is not the interface specification, but rather can be read to indicate any valid authorization rule can be interpretted by the system. It is designed so that it "reads" in a close approximation to English. The grammar is presented by means of syntax diagrams similar to the ones used by Jensen and Wirth[11] in their description of Pascal; these diagrams can be easily understood even by those who are not familiar with standard formalisms for defining grammars (regular expressions, Backus-Nauer form, etc.). The syntax diagrams are ordered so that the lowest-level objects are defined first. The diagrams appear in Figures 1-6. The ovals in them represent terminal symbols, while the boxes represent diagrams identified by the enclosed names. An example appears in Figure 7.

The grammar shown in Figures 1-6 is largely self-contained. Nonetheless, a short description of a few of the constructs (hyphenated terms refer to the syntax diagram) will help clarify the grammar:

- o Tokens. A token is a string of characters that could represent a valid name as determined by the NS.

- o Users. Users are names of users who have mailboxes (and are therefore known to the NS). Users who may authorize messages are explicitly declared.

- o Keywords. Authorization keys are keywords used by an organization to refer to message topics. An authorization rule can then pick authorizing agents that are appropriate for each topic declared to the system.

- o Access-Names. An access name is used to identify locations in the authorization rules where certain users can add new rules. These names appear first in an include declaration and subsequently in an include statement. A given access name that has been declared can appear only in one include statement. Include statements allow selected users to modify the authorization rules. The rules are primarily expressed in a "for" statement (this will be described below), and an include statement may restrict the modifiers that may appear in the "for" statement.

- o Authorization Procedure. An authorization procedure is a logical and temporal sequence of authorizing agents that are to be asked to approve a message. In this context, authorizing agents are users (these must be declared in an agent declaration statement to be described below) that have the capability to authorize messages, and that may or may not be allowed to modify a message (there is also a default obtained from the agent declaration).

- o Authorization procedure identifier declaration. On occasion it is useful to refer to an authorization procedure by a symbolic name. These names are established with a "define" clause, in which a symbolic name is given to an authorization procedure. To use a previously defined symbolic name in an authorization procedure, the name is prefaced with the keyword "use."

- o Time-Declaration. This statement identifies the users (these do not have to appear in the agent declaration) who can override the authorization rules if time limits are exceeded.

- o Statements. Statements select the authorization procedure that will be used for a given message. Each statement (including all those in begin-end blocks) is read in sequence until one is found that matches a message. An authorization procedure always matches, and an "always" authorization procedure statement "and"s its agent list with whatever agent lists subsequently match. If no statement following an "always" statement matches, the authorization procedure in the "always" statement matches. A "for" statement selects the statement following the keyword "do" if the sender, recipient,authorization key, precedence, or security

level of the message is the one given before the keyword "do" in the "for" statement. An "ask" statement provides for indirection (this statement matches whenever an authorization procedure would have matched): the authorization procedure following the keyword "ask" supplies authorizing agents who are to be asked to state the authorization procedure the message will use. Finally, the "time limit" statement fixes the time during which subsequently matched authorization procedures may be employed. If the time limit is exceeded and there is a "passed" clause, the statements therein are searched for a valid rule. If the time limit is exceeded and there is either no passed clause or no rule matched in the "passed" clause, the authorization service may then be authorized (if the sender has such a capability); otherwise it continues until an abort request is obtained from the sender.

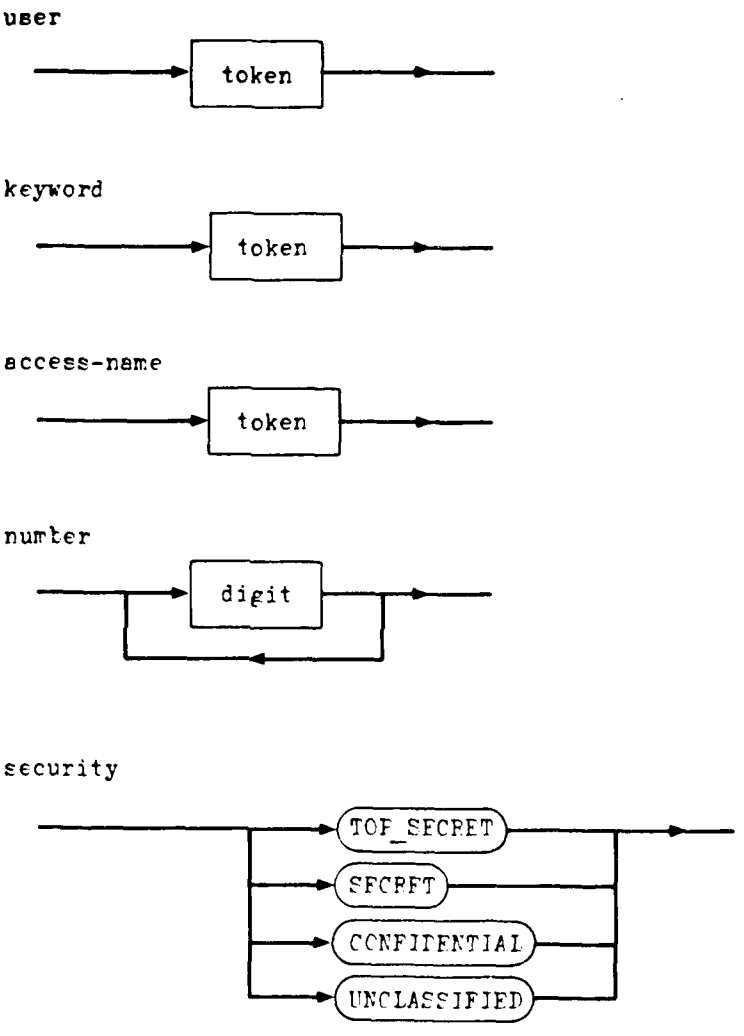
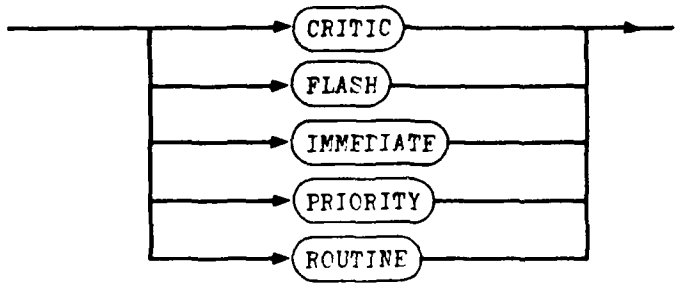
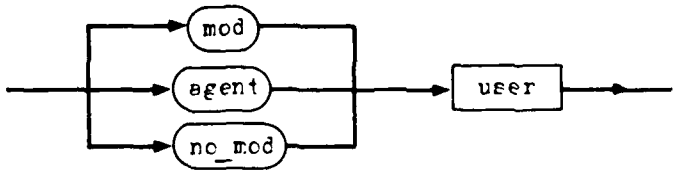


Figure A-1. Authorization Grammar Syntax Diagram

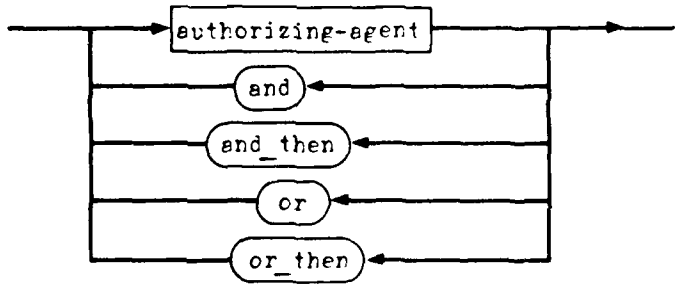
precedence



authorizing-agent



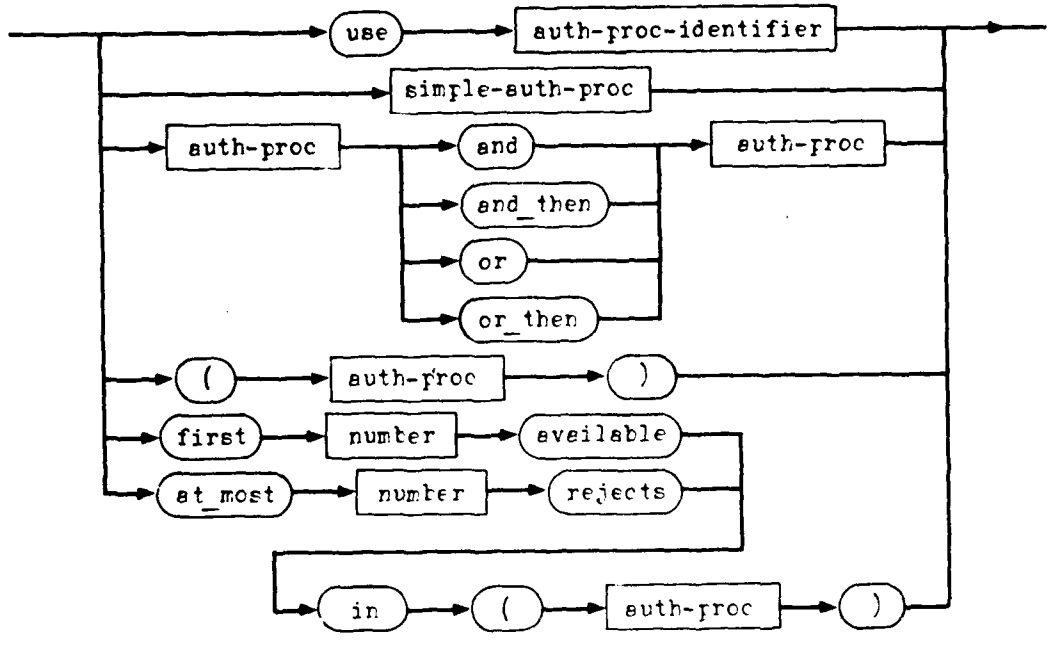
simple-authorization-procedure (simple-auth-proc)



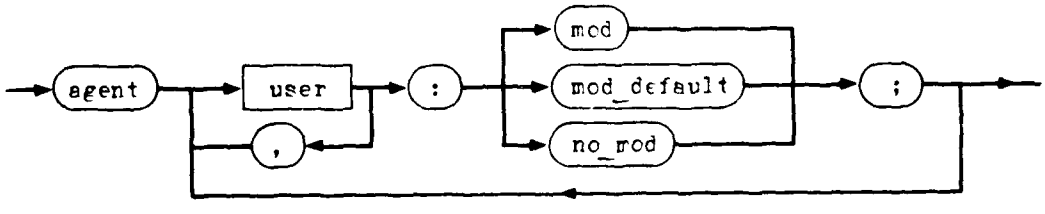
authorization-procedure-identifier (auth-proc-identifier)

Figure A-2. Authorization Grammar Syntax Diagram

authorization-procedure (*auth-proc*)



agent-declaration



keyword-declaration

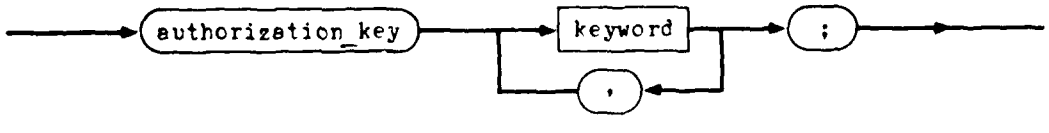
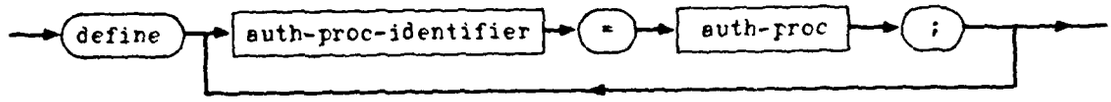
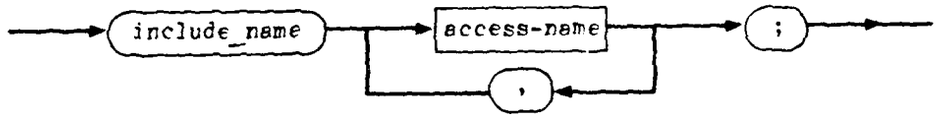


Figure A-3. Authorization Grammar Syntax Diagram

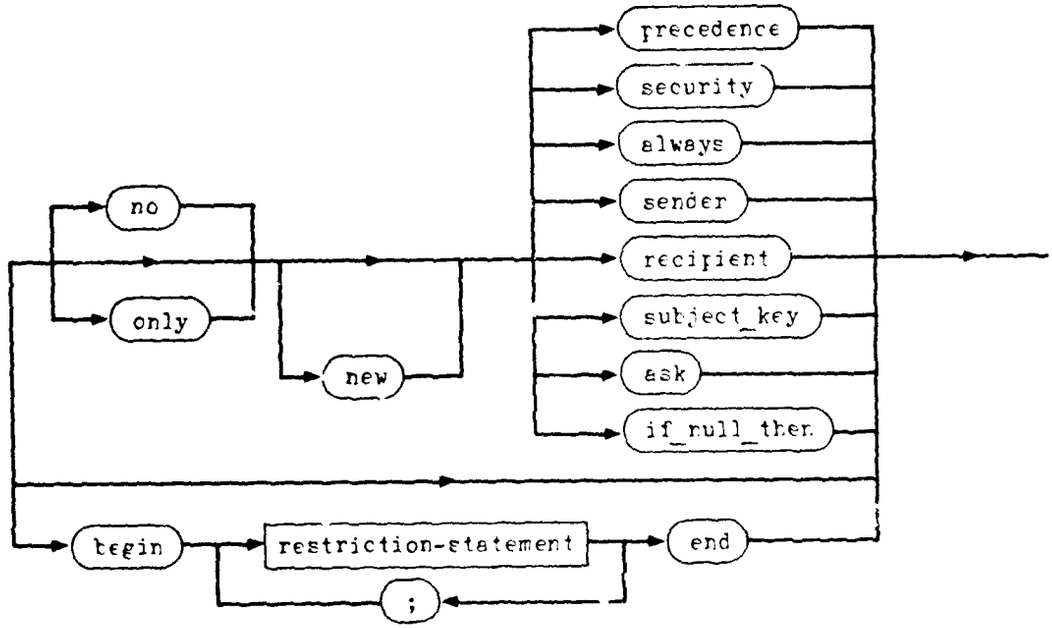
authorization-procedure-identifier-declaration (auth-proc-identifier-...)



include-declaration



restriction-statement



time-declaration

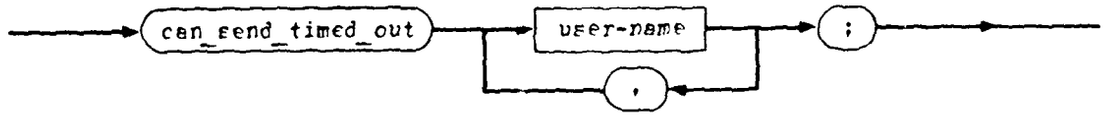


Figure A-4. Authorization Grammar Syntax Diagram

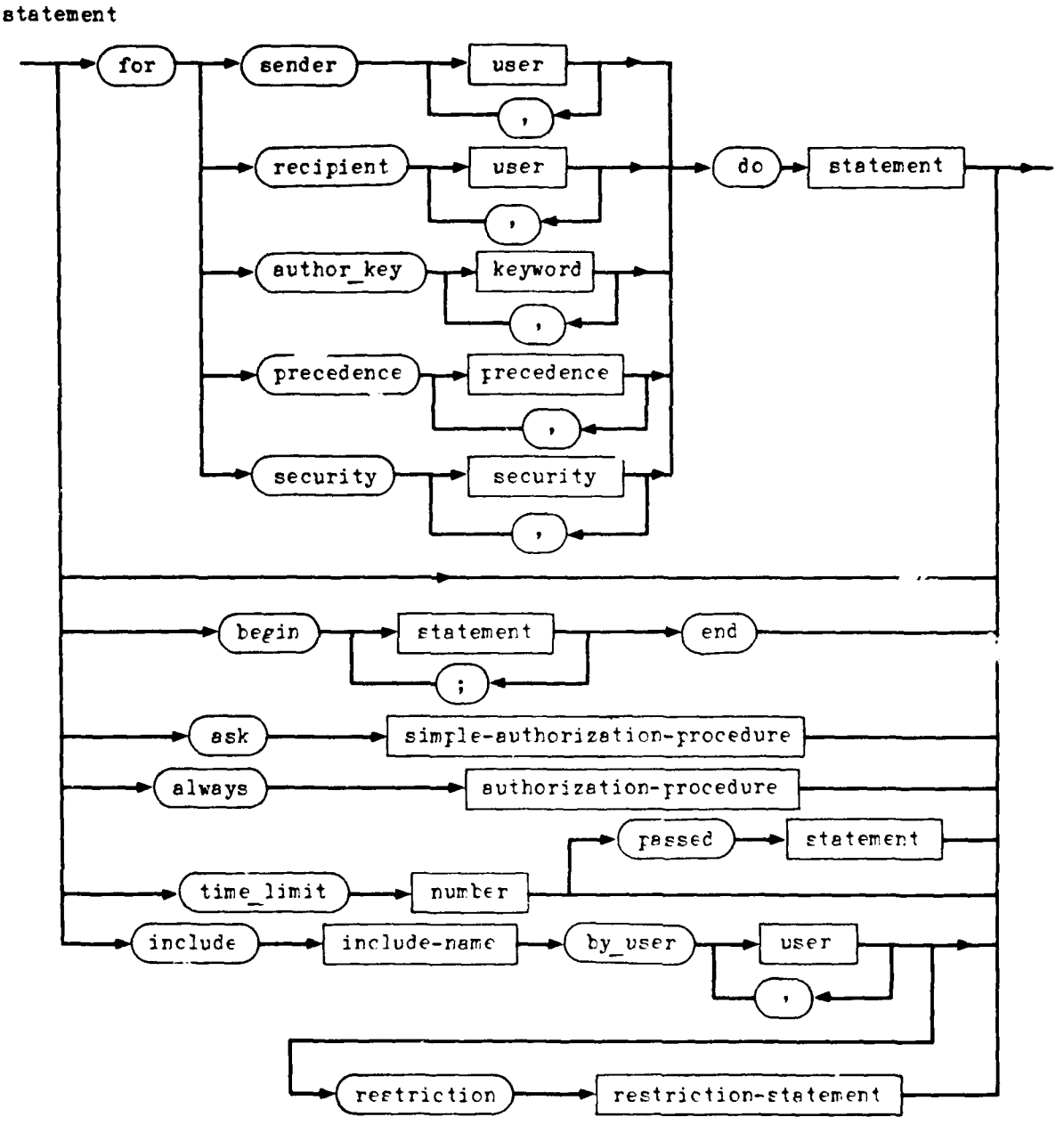


Figure A-5. Authorization Grammar Syntax Diagram

rules

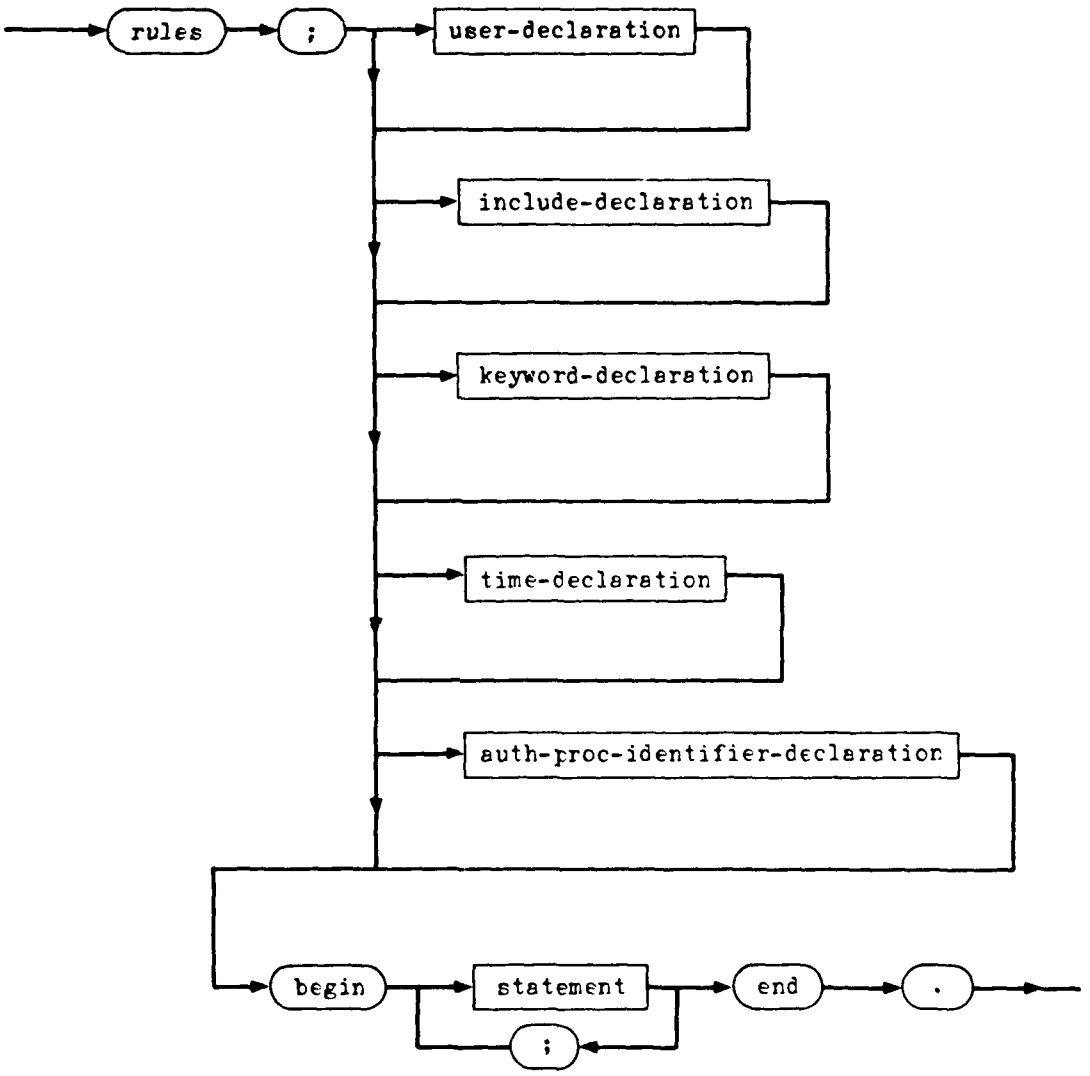


Figure A-6. Authorization Grammar Syntax Diagram

```
rules;
        user PN, KL: mod;
             WDE, ZS: no_mod;
             WTZ, EL: mod_default;

        include_name ADDITIONS;

        authorization_key  ABOUT_CASE_1, ABOUT_CASE_2;

        can_send_timed_out  BG, SR;

        define LIST_1 = (WTZ or EL) and_then (PN or KL);
               LIST_2 = first 2 available in ( WTZ or EL or WDE or ZS );
               LIST_3 = PN or KL;
        begin
                for security TOP_SECRET, SECRET do use LIST_3;

                for sender LM, LV do ask EL;

                for author_key ABOUT_CASE_1 do

                    begin
                        time_limit 30;
                        time_limit 20 passed ask WTZ;
                        for sender BG do use LIST_2 or_then use LIST_3;
                        for sender WTZ do mod EL;
                        for sender EL do mod WTZ;
                        for sender LM, LV do use LIST_1
                    end;

                for author_key ABOUT_CASE_2 do ask agent PN;

                include ADDITIONS by  PN, LK restriction
                                              only new sender;

        end.
```

Figure A-7. Authorization Rule Example

5. REFERENCES

1. C. L. Heitmeyer and S. H. Wilson, "Military Message Systems: Current and Future Directions," IEEE Transactions on Communications Vol. COM-28(9), pp. 1645-1654 (September 1980).

2. Charles Eldridge, Message Transfer Protocol Requirements Analysis, System Development Corporation (Sept. 25, 1981).

3. G. Bochmann and J. Pickens, A Methodology for the Specification of a Message Transport System, SRI International, Telecommunications Sciences Center (March 2, 1981).

4. CCITT Study Group 7 - Question 5, Message Handling Facilities - Model and Services - Version 1., May 1, 1981.

5. SRI Staff, DCEC Protocols Standardization Program: Message Transfer Protocol (Initial Version), System Development Corporation (December 1981).

6. International Organization for Standardization, "Data Processing -- Open Systems Interconnection -- Basic Reference Model," Computer Networks Vol. 5, pp. 81-118 (1981).

7. SYTEK Staff, DCEC Protocols Standardization Program: Preliminary Architecture Report, SDC (February 29, 1981).

8. J. B. Postel, "A Structured Format for Transmission of Multi-Media Messages," RFC 767, USC Information Sciences Institute (August 1980).

9. A. D. Birrell, R. Levin, R. M. Needham, and M. D. Schroeder, Grapevine, Xerox Palo Alto Research Center (April 1981).

10. J. R. Pickens, "Envelopes," MSA Note #4, SRI International, Telecommunications Science Center (February 1981).

11. Kathleen Jensen and Niklaus Wirth, Pascal User Manual and Report, Springer-Verlag, Berlin (1974).

PART II

MESSAGE TRANSFER PROTOCOL

1. OVERVIEW

1.1 INTRODUCTION

A computer based message system (CBMS) provides for the creation, editing, formatting, addressing, validation, routing, delivery, and retrieval of messages within and between groups of individuals and organizations in disjoint space and time. A military message system (MMS) must provide additional functions involving security and precedence, authorization and authentication, and interoperability with a variety of existing systems that were designed before the introduction of layered architectures. There is also an important distinction that must be made between formal and informal messages[1]. Informal messages provide a communication channel between individuals, whereas formal messages provide for official, authorized messages between organizations. Furthermore, since multimedia capabilities may eventually be added to message systems, the architecture of the message system should facilitate such enhancements. These requirements, viewed from the user's perspective, are presented in a Systems Development Corporation document[2] prepared in conjunction with the CBMS specified here.

The message transfer system consists of two layers--a presentation layer and a session layer--that lie atop of standard transport mechanisms. This document is concerned with the session layer, which runs the message transfer protocol (MTP). The MTP supplies message-transfer and facility connection services to the presentation layer. Since the latter may not be altered by the user, the MTP assumes that the layer above imposes sufficient controls upon the end user to prevent misuse of the message system. The MTP therefore ensures that only a validated presentation entity may use the MTP. The services provided by the MTP are designed to mesh with those required by the message presentation protocol (MPP), as described in the message presentation protocol specification document[3]. The MPP's primary function is to transfer messages between any of its users. However, because its users have to occasionally access remote facilities, connection services to such facilities are also furnished. The service description in this specification explicitly separates message transfer services from data base (or facility) access services, because it then becomes possible to access remote data bases (or facilities) with the aid of other protocols that may be available on a particular network (e.g., Telnet).

1.2 ARCHITECTURAL CONTEXT

The MTP fits within the session layer of the DoD architecture[4]. It enhances the basic services supplied by the transport layer in that alternative courses of action may be taken if a connection between message presentation entities (MPEs, the local instantiation of the MPP) is not possible, or if a connection fails during transmission. It is assumed that the transport (and lower) layers will supply at least the services available with TCP/IP. The MTP's most important function is to move messages from one message presentation entity to another. To do this, each message transfer entity (MTE, the instantiation of the protocol resident on a given host) takes a set of MPE addresses (these are assumed to be determined by the MPEs) uses then to establish a communication channel to other MPEs, and then transfers the message. There may

be several alternative addresses for each receipient. These are tried in order until one is found to which a connection is possible. The MTP also passes status and error messages to the user of the protocol indicating whether or not a message was sent, a connection could be completed, and so forth.

1.3 SCENARIOS

The following scenarios illustrate some of the functions performed by the MTP and some of the sequences of service requests (and responses thereto) that might occur.

- o Scenario 1.
  1. At the request of a user (i.e., an MPE), a connection is established with another MPE.
  2. A message is transferred over this connection to the recipient.
  3. The connection is closed.
- o Scenario 2.
  1. A user requests that a message be sent to the first available user a list of users.
  2. If the first recipient (MPE) is unavailable, a connection is made to the second on the list.
  3. Data transfer begins, but the connection fails during transmission.
  4. The MTE again attempts to connect with the first recipient on the list. This connection cannot be established; however, the third alternative is viable, and a connection is established.
  5. The message is transferred to the new recipient.
  6. The connection is closed.
  7. The recipient sends a reply to the originator indicating the status of the original message.
- o Scenario 3
  1. The originator requests that a message be transferred to several independent recipients.
  2. Scenario 1 or Scenario 2 occurs for each individual recipient selected.
- o Scenario 4.

1. The originator requests that a message be sent.

2. The lower layers cannot establish a connection

3. An error message is returned to the originator.

2. SERVICES SUPPLIED TO THE LAYER ABOVE

The MTP supplies transfer services to MPEs as described below.

2.1 MULTIPLE USERS

Although normally each MTE supplies services to only one user (e.g., one MPE), at some installations, multiple users may share a single MTE, thereby allowing several organizations to share a host for messaging support and still maintain separate administrative control of (the organization's) mail system policies and facilities.

2.2 VALIDATION SERVICES

Because the actual transfer of messages is done by the lower layers, the latter must ensure that only a legitimate MPE will use them for mail system purposes. This is necessary for example, to prevent a user agent from bypassing the administrative controls supplied by the MPE. Similarly, each session entity must know the identity of the peer entities with which it communicates, and must make sure that these entities are indeed authorized for mail system use.

2.3 AUTHORIZATION SERVICES

Although formal message authorization is primarily an MPE function, some support from the lower layers is necessary, as such authorization may require the coordination of several MPEs.

2.4 TRANSFER SERVICES

Transfer services, when provided with the internet address of MPEs, move messages from one MPE to another. The basic service is a "send" service. The "send" service must be given a message with an overall security level, a precedence level, and a list of recipients. As viewed from the lower layers, each recipient consists of a security level, a precedence, and a series of alternative addresses (one or more). The service attempts to send mail to the first of these addresses, trying the second address only if mail cannot be delivered to the first--and so on through the entire series, if necessary. The MPE address given to the service is not necessarily that of the recipient; however, if a message is to be passed farther along the network (i.e., to another MPE), this is the responsibility of the MPEs, not the MTP.

A "send" service can be invoked with a variety of options:

- o Normal Transmission. A message is transferred through a reliable transport mechanism to a remote MPE.
- o Source Routing. The user of the protocol may specify the route with whatever level of control the transport mechanism allows.
- o Error Conditions. If none of the MPEs specified in the address list can be reached, or if there is a failure during transmission from which the

lower layers cannot recover, the "send" service returns an error indication to the user of the protocol.

- o Security. The lower layer checks that the security level requested for a message matches that requested from the transport mechanism.

- o Precedence. Several of precedence levels may be specified. These include ECP/CRITIC, FLASH, PRIORITY, ROUTINE.

2.5 NAME SERVER ACCESS SERVICES

This service allows access to remote NSs. The MPE may request services from a remote NS, but may not make changes in the NS's data base. If a remote NS cannot be accessed, or if there is a failure, appropriate error indications are returned.

2.6 STATUS-REPORTING SERVICES

Status-reporting services allow for the transfer of delivery acknowledgments and status messages between MPEs. Different grades of service may be requested, depending on whether or not an occasional loss of one these messages is acceptable.

2.7 ARCHIVE ACCESS SERVICE

Archive access services enables an MPE to connect with a remote MPE to access the latter's archival services. These services allow one to request services from remote archival facilities, i.e., to retrieve archived messages or to interrogate an archive's data base when that archive is not available on a local host. Generally, these services are used to access long-term archives, such as those that might be maintained at a central facility.

3. SERVICES TO BE PROVIDED BY THE LOWER LAYERS

The MTP requires transport services, such as those supplied by TCP, that provide a reliable link between MPEs. Although TCP is adequate for most mail system messages, in some cases (e.g., certain status messages), a less reliable, connectionless service may suffice.

3.1 CONNECTION-BASED SERVICES

The MTP requires a transport service that provides a reliable, private communication channel for a pair of MTEs. The lower layer must allow an MTE to request various grades of service--at least precedence and security levels. This service ideally should have an error rate of less than one error in 10**12. It should provide the following:*

- o Multiple Communication Channels. The service should allow simultaneous communication channels to multiple MTEs.

- o Connection Establishment. The service should allow a communication channel between MPEs to be established. An MPE must have suitable support so as to be able to restrict these channels to authorized MPEs.

- o Connection Termination. The service should be able to terminate a connection either gracefully (with no loss of data) or abruptly (regardless of data loss). If the connection is aborted, both MTEs must be informed.

- o Data Transport. The service shall provide for the transport of data. This transport is error-free (with high probability), timely (within a delivery time specified by the MTP), ordered (in the same sequence as provided by the originating MTE), labeled (each communication channel will have a security and precedence level associated with it), and flow-controlled (the flow of data across the channel shall be regulated to prevent service degradation and failure). Transport services over an established channel shall have the following capabilities:

  - Data Stream Partitioning: The transport service shall allow an MTE to indicate places in the data stream signifying that preceding data should be delivered without delay.

  - Urgent-Data Signaling: The transport service shall allow a sending MTE to inform a receiving MTE of the presence and location of significant data in the forthcoming data stream.

- o Error reports. The service must report errors for which it cannot compensate. These include host failure, internetwork partitioning, subnetwork failure, and internetwork failure.

---

* These provisions are paraphrased from a TCP specification[5] for maintaining compatibility with TCP-based transport layers.

3.2 CONNECTIONLESS SERVICES

Although connection-based services suffice for message-system functions, some MTE services may be better implemented with connectionless services. The MTE services that may benefit from using connectionless services are those for which high reliability is not required. For example, some status messages and information requests do not need the reliability appropriate for message transfer.

4. REFERENCES

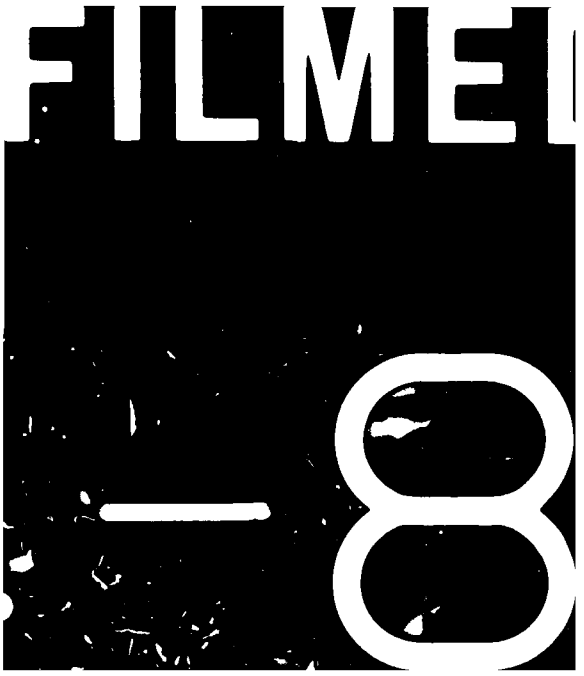
1. C. L. Heitmeyer and S. H. Wilson, "Military Message Systems: Current and Future Directions," IEEE Transactions on Communications Vol. COM-28(9), pp. 1645-1654 (September 1980).

2. Charles Eldridge, Message Transfer Protocol Requirements Analysis, System Developement Corporation (Sept 25, 1981).

3. SRI Staff, DCEC Protocol Standardization Program: Message Presentation Protocol (Initial Version), System Development Corporation (December 1981).

4. SYTEK Staff, DCEC Protocols Standardization Program; Preliminary Architecture Report, SDC (February 29, 1981).

5. Mary Bernstein, DCEC Protocols Standardization Program; TCP Standard: Initial Version, System Development Corporation (July 16, 1981).


FILME
8